Fermat quotients: Exponential sums, value set and primitive roots

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

January 20, 2013

Abstract

For a prime p and an integer u with $\gcd(u, p) = 1$, we define Fermat quotients by the conditions

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \pmod p, \qquad 0 \le q_p(u) \le p - 1.$$

D. R. Heath-Brown has given a bound of exponential sums with N consecutive Fermat quotients that is nontrivial for $N \ge p^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$. We use a recent idea of M. Z. Garaev together with a form of the large sieve inequality due to S. Baier and L. Zhao, to show that on average over p one can obtain a nontrivial estimate for much shorter sums starting with $N \ge p^{\varepsilon}$. We also obtain lower bounds on the image size of the first N consecutive Fermat quotients and use it to prove that there is a positive integer $n \le p^{3/4+o(1)}$ such that $q_p(n)$ is a primitive root modulo p.

Keywords: Fermat quotient, exponential and character sum, large sieve inequality, primitive root

Mathematics Subject Classification (2010): 11A07, 11L40, 11N35

1 Introduction

1.1 Previous results

For a prime p and an integer u with $\gcd(u,p) = 1$ the *Fermat quotient* $q_p(u)$ is defined as the unique integer with

$$q_p(u) \equiv \frac{u^{p-1}-1}{p} \pmod p, \qquad 0 \le q_p(u) \le p-1.$$

Fermat quotients appear and play a very important role in a variety of problems, see [8, 11, 12, 15, 19, 21] and references therein.

In particular, Heath-Brown [14] has considered the exponential sums

$$S_p(a;N) = \sum_{\substack{n=1\\ gcd(n,p)=1}}^{N} \mathbf{e}_p(aq_p(n)), \qquad a \in \mathbb{Z},$$

where for an integer $r \ge 1$ and a real z we define $\mathbf{e}_r(z) = \exp(2\pi iaz/r)$, and noticed that using the Pólya-Vinogradov and Burgess bounds (see [16, Theorems 12.5 and 12.6]) leads to the estimate

$$\max_{\gcd(a,p)=1} |S_p(a;N)| \le N^{1-1/\nu} p^{(\nu+1)/2\nu^2+o(1)} \tag{1}$$

with any fixed integer $\nu \ge 1$ (in fact in [14, Theorem 2] it is presented only with $\nu = 2$ but the argument applies to any ν, see also [8, Section 4]). It is easy to see that (1) is nontrivial for $N \ge p^{1/2+\varepsilon}$ with an arbitrary fixed $\varepsilon > 0$, but becomes trivial for $N \le p^{1/2}$. For longer intervals of length $N \ge p^{1+\varepsilon}$, a nontrivial bound of exponential sums with linear combinations of $s \ge 1$ consecutive values $q_p(u), \ldots, q_p(u+s-1)$ has been given in [21], see also [7] for a generalisation. Several one-dimensional and bilinear multiplicative character sums, as well as sums over primes, with Fermat quotients have recently been estimated in [22, 23]. In particular, by [22, Theorem 3.1], for any nontrivial multiplicative character η modulo p, we have

$$\left| \sum_{\substack{n=1\\ gcd(n,p)=1}}^{N} \eta(q_p(n)) \right| \le N^{1-1/\nu} p^{(5\nu+1)/4\nu^2+o(1)} \tag{2}$$

with any fixed integer $\nu \geq 1$. Furthermore, Gomez and Winterhof [10] have estimated multiplicative character sums with the s-fold products $q_p(n+d_1)\dots q_p(n+d_s)$ over intervals of length $N \geq p^{3/2+\varepsilon}$ for any fixed $\varepsilon > 0$. In turn, the bound of [10] has been used by Aly and Winterhof [1] to study some Boolean functions associated with Fermat quotients.

The image size

$$I_p(N) = \#\{q_p(n) \ : \ 1 \leq n \leq N, \ \gcd(n,p) = 1\}$$

of the first N Fermat quotients, has also been studied. We note that since $q_p(1) = 0$, the smallest N with $I_p(N) > 1$, that is frequently denoted by ℓ_p, corresponds to the smallest nonzero Fermat quotient and has been studied in a number of works, see [4, 11, 12, 15, 19]. It is also shown in [24] that for any fixed $\varepsilon > 0$ and sufficiently large p, we have $I_p(N) = p$ for $N \geq p^{463/252+\varepsilon}$ and $I_p(N) = p + o(p)$ for $N \geq p^{3/2+\varepsilon}$.

Most of these above results depend on the following well-known property of Fermat quotients:

$$q_p(uv) \equiv q_p(u) + q_p(v) \pmod p, \tag{3}$$

see, for example, [8, Equation (3)], which is also used here.

1.2 Our results

Here we show that on average over primes p one can obtain a stronger bound than (1), which is nontrivial for $N \geq p^{\varepsilon}$. This result is based on a combination of the idea of Heath-Brown [14] to interpret the sums $S_p(a;N)$ as multiplicative character sums with the approach of Garaev [9] of estimating the maximal value of such sums via the large sieve inequality. However, here instead of the classical form of the large sieve inequality, used in [9], we use the version of Baier and Zhao [3], where the averaging is taken over square moduli. Our proof follows quite close to that of [9, Theorem 3] however we allow the length of the corresponding sums to vary with the modulus. In fact our argument gives a bound on the sums with arbitrary primitive characters modulo p^2, not necessary of order p as in the case of Fermat quotients, see (10) below.

However here we use some ideas of [21] to obtain new lower bounds on the image size $I_p(N)$. More precisely, we study the values of N for which $I_p(N)$ grows as a power of p. So our results somewhat interpolate between those

of [4], where the case $I_p(N) > 1$ has been studied, and of [24] addressing case of very large values of $I_p(N)$. In turn these estimates are used to estimate the smallest primitive root in the sequence of Fermat quotients.

We note that the bound (2), taken with a sufficiently large ν, implies that there exists a positive integer $n \le p^{5/4+o(1)}$ such that $q_p(n)$ is a primitive root modulo p. Here we use our lower bounds on $I_p(N)$ and also bounds of double character sums to improve this estimate (and replace exponent $5/4$ with $3/4$).

1.3 Notation

Throughout the paper, p always denotes a prime number, while k, m and n (in both the upper and lower cases) denote positive integer numbers.

The implied constants in the symbols 'O', '$\ll$' and '$\gg$' may occasionally depend on the integer parameter $\nu \ge 1$ and the t real parameter $\varepsilon > 0$, and are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the assertion that the inequality $|U| \le cV$ holds for some constant $c > 0$.

Finally, the notation $z \sim Z$ means that z must satisfy the inequality $Z < z \le 2Z$.

2 Preparations

2.1 Basics on exponential and character sums

We recall, that for any integers z and $r \ge 1$, we have the orthogonality relation

$$\sum_{-r/2 \le b < r/2} \mathbf{e}_r(bz) = \begin{cases} r, & \text{if } z \equiv 0 \pmod r, \\ 0, & \text{if } z \not\equiv 0 \pmod r, \end{cases} \tag{4}$$

see [16, Section 3.1].

We also need the bound

$$\sum_{n=K+1}^{K+L} \mathbf{e}_r(bn) \ll \min\left\{L, \frac{r}{|b|}\right\}, \tag{5}$$

which holds for any integers b, K and $L \ge 1$ with $0 < |b| \le r/2$, see [16, Bound (8.6)].

We also refer to [16, Chapter 3] for a background on multiplicative characters.

The link between multiplicative characters and exponential sums is given by the following well-known identity (see [16, Equation (3.12)]) involving Gauss sums

$$\tau_r(\chi) = \sum_{v=1}^{r} \chi(v)\, \mathbf{e}_r(v)$$

defined for a character χ modulo an integer $r \geq 1$:

Lemma 1. *For any multiplicative character χ modulo r and an integer b with $\gcd(b, r) = 1$, we have*

$$\chi(b)\tau_r(\overline{\chi}) = \sum_{v=1}^{r} \overline{\chi}(v)\, \mathbf{e}_r(bv),$$

where $\overline{\chi}$ is the complex conjugate character to χ.

By [16, Lemma 3.1] we also have:

Lemma 2. *For any primitive multiplicative character χ modulo r we have*

$$|\tau_r(\chi)| = r^{1/2}.$$

As usual, we use $\mu(d)$ and $\varphi(d)$ to denote the Möbius and the Euler functions of an integer $d \geq 1$, respectively. We now mention the following well-known characterisation of primitive roots modulo p which follows from the inclusion-exclusion principle and the orthogonality property of characters (see, for example, [20, Excercise 5.14]).

Lemma 3. *For any integer a, we have*

$$\frac{p-1}{\varphi(p-1)} \sum_{d \mid p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord} \eta = d} \eta(a) = \begin{cases} 1, & \text{if } a \text{ is a primitive root modulo } p, \\ 0, & \text{otherwise,} \end{cases}$$

where the inner sum is taken over all $\varphi(d)$ multiplicative characters modulo p of order d.

2.2 Double sums of multiplicative characters

We now recall a result of A. A. Karatsuba, see [17] or [18, Chapter VIII, Problem 9].

Lemma 4. *For any nontrivial character η modulo p, and arbitrary sets $\mathcal{A}, \mathcal{B} \subseteq \{0, 1, \ldots, p-1\}$, we have*

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\eta(a+b)\right| \ll (\#\mathcal{A})^{1-1/2\nu}\#\mathcal{B}p^{1/4\nu} + (\#\mathcal{A})^{1-1/2\nu}(\#\mathcal{B})^{1/2}p^{1/2\nu}$$

with any fixed integer $\nu \geq 1$.

2.3 Sums $S_p(a; N)$ and multiplicative character sums

Heath-Brown [14] has noticed that (3) implies that the sums $S_p(a; N)$ are essentially sums of multiplicative characters:

Lemma 5. *For any integer a with $\gcd(a, p) = 1$ there is a primitive multiplicative character χ modulo p^2 such that*

$$S_p(a; N) = \sum_{n=1}^{N}\chi(n).$$

We note that the character χ of Lemma 5 is of order p, however we do not use this property.

2.4 Large sieve for square moduli

We make use of the following version of the large sieve inequality for square moduli which is due to Baier and Zhao [3, Theorem 1]:

Lemma 6. *Let $\alpha_1, \ldots, \alpha_K$ be an arbitrary sequence of complex numbers and let*

$$A = \sum_{k=1}^{K}|\alpha_n|^2 \qquad \text{and} \qquad T(u) = \sum_{k=1}^{K}\alpha_n\exp(2\pi iku).$$

Then, for any fixed $\varepsilon > 0$ and arbitrary $R \geq 1$, we have

$$\sum_{1\leq r\leq R}\sum_{\substack{a=1\\ \gcd(a,r)=1}}^{r^2}\left|T(a/r^2)\right|^2 \ll (RK)^{\varepsilon}\left(R^3 + K + \min\{KR^{1/2}, K^{1/2}R^2\}\right)A.$$

2.5 Ratios of small height in multiplicative subgroups of residue rings

Let $\mathcal{G}$ be a multiplicative subgroup of the group of units in the residue ring modulo an integer $m \ge 1$. Also, for a real Z, let $N(m, \mathcal{G}, Z)$ be the number of solutions to the congruence

$$wx \equiv y \pmod{m}, \qquad \text{where } 0 < |x|, |y| \le Z,\ w \in \mathcal{G}.$$

We now recall [5, Theorem 1] which gives an upper bound on $N(m, \mathcal{G}, Z)$. We note that the proof given in [5] works only for $Z \ge m^{1/2}$ (which is always satisfied in the present paper); however it is shown in [6] that the result holds without this condition too, exactly as it is formulated in [5].

Lemma 7. *Let $\nu \ge 1$ be a fixed integer and let $m \to \infty$. Assume $\#\mathcal{G} = t \gg \sqrt{m}$. Then for any positive number Z we have*

$$N(m, \mathcal{G}, Z) \le Zt^{(2\nu+1)/2\nu(\nu+1)} m^{-1/2(\nu+1)+o(1)} + Z^2 t^{1/\nu} m^{-1/\nu+o(1)}.$$

3 Main Results

3.1 Bound of exponential sums on average

Let P and $N \le P^2$ be two sufficiently large positive integers. Assume that for every $p \sim P$ we are given an integer $N_p \sim N$.

Theorem 8. *For every fixed integer $\nu \ge 1$, we have*

$$\sum_{p \sim P} \max_{\gcd(a,p)=1} |S_p(a, N_p)|^{2\nu} \le \left(P^3 + N^\nu + \min\{N^\nu P^{1/2}, N^{\nu/2} P^2\}\right) N^\nu P^{o(1)}$$

for any sequence $N_p \sim N$, as $P \to \infty$.

Proof. We follow the ideas of Garaev [9, Theorem 3].

Using Lemma 5, for each $p \sim N$ we choose a multiplicative character χ_p modulo p^2 such that

$$\max_{\gcd(a,p)=1} |S_p(a; N_p)| = \left| \sum_{n=1}^{N_p} \chi_p(n) \right|. \tag{6}$$

Let $M = 2N$. Using (4), for $N_p \sim N$ we write

$$\begin{aligned}\sum_{n=1}^{N_p} \chi_p(n) &= \sum_{m=1}^{M} \chi_p(m) \frac{1}{M} \sum_{n=1}^{N_p} \sum_{b=-N}^{N-1} \mathbf{e}_M(b(m-n)) \\ &= \frac{1}{M} \sum_{b=-N}^{N-1} \sum_{n=1}^{N_p} \mathbf{e}_M(-bn) \sum_{m=1}^{M} \chi_p(m)\, \mathbf{e}_M(bm).\end{aligned}$$

Recalling (5), we derive

$$\left| \sum_{n=1}^{N_p} \chi_p(n) \right| \ll \sum_{b=-N}^{N-1} \frac{1}{|b|+1} \left| \sum_{m=1}^{M} \chi_p(m)\, \mathbf{e}_M(bm) \right|.$$

Therefore, writing $|b| = |b|^{(2\nu-1)/2\nu} |b|^{1/2\nu}$, the Hölder inequality yields the bound

$$\left| \sum_{n=1}^{N_p} \chi_p(n) \right|^{2\nu} \ll (\log N)^{2\nu-1} \sum_{b=-N}^{N-1} \frac{1}{|b|+1} \left| \sum_{m=1}^{M} \chi_p(m)\, \mathbf{e}_M(bm) \right|^{2\nu}.$$

Thus, by (6) we obtain

$$\sum_{p \sim P} \max_{\gcd(a,p)=1} |S_p(a, N_p)|^{2\nu} \ll (\log N)^{2\nu-1} \sum_{b=-N}^{N-1} \frac{1}{|b|+1} U_b, \tag{7}$$

where

$$U_b = \sum_{p \sim P} \left| \sum_{m=1}^{M} \chi_p(m)\, \mathbf{e}_M(bm) \right|^{2\nu}.$$

We now note that

$$\left(\sum_{m=1}^{M} \chi_p(m)\, \mathbf{e}_M(bm) \right)^{\nu} = \sum_{k=1}^{K} \rho_{b,\nu}(k) \chi_p(k),$$

where $K = M^{\nu}$ and

$$\rho_{b,\nu}(k) = \sum_{\substack{m_1,\ldots,m_\nu=1 \\ m_1 \ldots m_\nu = k}}^{M} \mathbf{e}_M(b(m_1 + \ldots + m_\nu)).$$

Using Lemma 1, we write

$$\left(\sum_{m=1}^{M} \chi_p(m)\, \mathbf{e}_M(bm)\right)^{\nu} = \sum_{k=1}^{K} \rho_{b,\nu}(k) \frac{1}{\tau_{p^2}(\overline{\chi}_p)} \sum_{v=1}^{p^2} \overline{\chi}_p(v)\, \mathbf{e}_{p^2}(kv).$$

Changing the order of summation, by Lemma 2 and the Cauchy inequality, we obtain,

$$\left|\sum_{m=1}^{M} \chi_p(m)\, \mathbf{e}_M(bm)\right|^{2\nu} \le \sum_{v=1}^{p^2} \left|\sum_{k=1}^{K} \rho_{b,\nu}(k)\, \mathbf{e}_{p^2}(kv)\right|^2.$$

Therefore

$$U_b = \sum_{p\sim P} \sum_{v=1}^{p^2} \left|\sum_{k=1}^{K} \rho_{b,\nu}(k)\, \mathbf{e}_{p^2}(kv)\right|^2.$$

Using the standard bounds on the divisor function, see [16, Bound (1.81)] we conclude that

$$|\rho_{b,\nu}(k)| \le \sum_{m_1 \ldots m_\nu = k} 1 = k^{o(1)}$$

as $k \to \infty$. Hence, we now derive from Lemma 6

$$U_b \le \left(P^3 + N^\nu + \min\{N^\nu P^{1/2}, N^{\nu/2} P^2\}\right) N^\nu P^{o(1)},$$

which after substitution in (7) concludes the proof. □

In particular, taking a sufficiently large ν, we obtain a nontrivial bound on average of very short sums.

Corollary 9. *For any fixed $\varepsilon > 0$ and $\delta > 0$ there exists $\kappa > 0$ such that for all $p \sim P$ except for $O(P^{1/2+\delta})$ of them, we have*

$$\max_{\gcd(a,p)=1} |S_p(a, N_p)| \le N_p p^{-\kappa},$$

for any sequence $N_p \sim N$, with some $N \ge P^\varepsilon$.

Proof. Taking $\nu = \lceil 3/\varepsilon \rceil$, we obtain from Theorem 8

$$\sum_{p\sim P} \max_{\gcd(a,p)=1} |S_p(a, N_p)|^{2\nu} \le N^{2\nu} P^{1/2+o(1)}.$$

So for $\kappa = 0.9\delta/\nu$, we see that the inequality

$$\max_{\gcd(a,p)=1} |S_p(a, N_p)| > N_p p^{-\kappa}$$

holds for at most $P^{1/2+\nu\kappa+o(1)} = O(P^{1/2+\delta})$ primes $p \sim P$. □

Furthermore, taking $\nu = 3$ we derive

Corollary 10. *For any fixed $\varepsilon > 0$ there exists $\delta > 0$ such that for all $p \sim P$ except for $O(P^{1-\delta})$ of them, we have*

$$\max_{\gcd(a,p)=1} |S_p(a, N_p)| \le N_p p^{-1/12+\varepsilon},$$

for any sequence $N_p \sim N$, with some $N \ge P^{5/6}$.

We note that the bound of Corollary 10 is stronger than that of (1) for $N \le p^{10/11}$.

3.2 Image size

Here we give some lower bounds on the image size $I_p(N)$.

First we consider the case of large values of N, for which use an argument of the proof of [21, Theorem 13].

Theorem 11. *For every p and $N < p$, we have*

$$I_p(N) \ge (1 + o(1))\frac{N^2}{p(\log N)^2}.$$

Proof. Let $Q_p(N, a)$ be the number of primes $\ell \in \{1, \ldots, N\}$ with $q_p(\ell) = a$. Clearly, by the prime number theorem

$$\sum_{a=0}^{p-1} Q_p(N, a) = (1 + o(1))\frac{N}{\log N}.$$

We now use the trivial estimate

$$\sum_{a=0}^{p-1} Q_p(N, a)^2 \le \sum_{a=0}^{p-1} Q_p(p-1, a)^2$$

and recall that by [21, Bound (17)] the last sum is $O(p)$.

Since by the Cauchy inequality we have

$$\left(\sum_{a=0}^{p-1} Q_p(N,a)\right)^2 \le I_p(N) \sum_{a=0}^{p-1} Q_p(N,a)^2,$$

the result now follows. □

For small values of N we use an argument similar to that of the proof of [21, Theorem 11].

Theorem 12. *For every p and arbirary fixed $\varepsilon > 0$ there exists some $\delta > 0$ such that for $p^\varepsilon < N < p$ we have*

$$I_p(N) \ge p^\delta.$$

Proof. Let

$$\mathcal{W}_p(N) = \{(u,v) \ : \ 1 \le u, v \le N, \ q_p(u) = q_p(v)\}.$$

We see from (3) that if $(u,v) \in \mathcal{W}_p(N)$ then for

$$w \equiv u/v \pmod{p^2} \tag{8}$$

we have

$$q_p(w) \equiv q_p(u) - q_p(v) \equiv 0 \pmod{p}.$$

Since all values of w with $q_p(w) \equiv 0 \pmod{p}$ and $\gcd(w,p) = 1$ satisfy

$$w^{p-1} \equiv 1 \pmod{p^2},$$

they are elements of the group $\mathcal{G}_p$ of the pth power residues modulo p^2. Thus we see from (8) that

$$\#\mathcal{W}(p) \le N(p^2, \mathcal{G}_p, N),$$

where $N(m, \mathcal{G}, Z)$ is as in Section 2.5. In particular, using Lemma 7 gives

$$\#\mathcal{W}(p) \le Np^{1/2\nu(\nu+1)+o(1)} + N^2 p^{-1/\nu+o(1)}.$$

Taking ν as the smallest integer that satisfies the inequality,

$$\frac{1}{2\nu(\nu+1)} \le \frac{\varepsilon}{2},$$

we obtain for this ν,

$$\#\mathcal{W}(p) \le N^{3/2+o(1)} + N^2 p^{-1/\nu+o(1)}.$$

Since

$$\sum_{a=0}^{p-1} R_p(N,a) = N \qquad \text{and} \qquad \sum_{a=0}^{p-1} R_p(N,a)^2 = \#\mathcal{W}(p),$$

where $R_p(N,a)$ is the the number of positive integers $n \le N$ with $q_p(n) = a$, as in the proof of Theorem 11, using the Cauchy inequality we derive the desired result. □

3.3 Smallest primitive roots

Our bound on the smallest primitive roots among the values of the Fermat quotients is based on the congruence (3), Lemma 4 and the results of Sections 3.2

Theorem 13. *For every p, there exists $n \le p^{3/4+o(1)}$ such that $q_p(n)$ is a primitive root modulo p.*

Proof. Let us fix some $\varepsilon > 0$ and put

$$U = \left\lceil p^{3/4+\varepsilon} \right\rceil \qquad \text{and} \qquad V = \left\lceil p^{\varepsilon} \right\rceil.$$

By Theorem 11 and Theorem 12, we have

$$I_p(U) \ge p^{1/2+\delta} \qquad \text{and} \qquad I_p(V) \ge p^{\delta},$$

respectively. Furthermore, let $\mathcal{U} \subseteq \{1,\ldots,U\}$ and $\mathcal{V} \subseteq \{1,\ldots,V\}$ satisfy $\#\mathcal{U} = \#\{q_p(u) \ : \ u \in \mathcal{U}\} = I_p(U)$ and $\#\mathcal{V} = \#\{q_p(v) \ : \ v \in \mathcal{V}\} = I_p(V)$, respectively.

Taking a sufficiently large ν in Lemma 4 we obtain that there is some $\kappa > 0$ depending only on δ (and thus only on ε) such that for any nontrivial character η modulo p, we have

$$\sum_{u\in\mathcal{U}} \sum_{v\in\mathcal{V}} \eta\left(q_p(u) + q_p(v)\right) \ll \#\mathcal{U}\#\mathcal{V}p^{-\kappa}. \tag{9}$$

Let T be the number of primitive roots of the form $q_p(u) + q_p(v)$ with $u \in \mathcal{U}$ and $v \in \mathcal{V}$. By Lemma 3, we have

$$\begin{aligned} T &= \frac{p-1}{\varphi(p-1)} \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \sum_{d \mid p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord} \eta = d} \eta\left(q_p(u) + q_p(v)\right) \\ &= \frac{p-1}{\varphi(p-1)} \sum_{d \mid p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord} \eta = d} \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \eta\left(q_p(u) + q_p(v)\right). \end{aligned}$$

Separating the contribution $(p-1)\#\mathcal{U}\#\mathcal{V}/\varphi(p-1)$ of the principal character and using (9), we derive

$$T = \frac{(p-1)\#\mathcal{U}\#\mathcal{V}}{\varphi(p-1)} \left(1 + p^{-\kappa} \sum_{d \mid p-1} 1\right).$$

Recalling the well-known estimates on the divisor function

$$\sum_{d \mid s} 1 = s^{o(1)}$$

as $s \to \infty$, see [13, Theorem 317], we obtain that $T > 0$. Thus there are $u \in \mathcal{U}$ and $v \in \mathcal{V}$ such that $q_p(u) + q_p(v)$ is a primitive root modulo p. Recalling (3) we see that for $n = uv \le UV \le 2p^{3/4+2\varepsilon}$ the Fermat quotient $q_p(n)$ is a primitive root modulo p.

Since ε is arbitrary, the result now follows. □

In particular, we see that for any $d \mid p-1$ there is a small dth power nonresidue modulo p (that is, an integer which is not a dth power modulo p) among Fermat quotients.

Corollary 14. *For every p and positive integer $d \mid p-1$ there exists $n \le p^{3/4+o(1)}$ such that $q_p(n)$ is a dth power nonresidue modulo p.*

4 Comments

We remark that a full analogue of (1) also holds for sums over shifted intervals $[L+1, L+N]$ uniformly over L. However, the method of proof of Theorem 8 applies only to initial intervals.

We also notice that taking ν slowly growing with p and estimating $\rho_{b,\nu}(k)$ more carefully, as in [9], one can obtain bounds on average of even shorter sums than in Corollary 9. Also as in [9], one can estimate short exponential sums of Fermat quotients taken over primes ℓ rather than over consecutive integers. Note that no "individual" bound of such sums is known.

Clearly, our results apply to sums of arbitrary primitive characters modulo p^2 giving, for every fixed integer $\nu \ge 1$, the bound

$$\sum_{p \sim P} \max_{\chi \in \mathcal{X}_p^*} \left| \sum_{n=1}^{N_p} \chi(n) \right|^{2\nu} \le \left(P^3 + N^\nu + \min\{N^\nu P^{1/2}, N^{\nu/2} P^2\}\right) N^\nu P^{o(1)}, \quad (10)$$

where $\mathcal{X}_p^*$ is the set of primitive multiplicative characters modulo p^2, for any sequence $N_p \sim N$, as $p \to \infty$. Using the results of [2] one can also obtain similar (albeit weaker) estimates modulo p^k with an arbitrary fixed $k \ge 2$.

Furthermore, it has been conjectured by Zhao [25] (see also [3]) that the bound of Lemma 6 holds in the form

$$\sum_{1 \le r \le R} \sum_{\substack{a=1 \\ \gcd(a,r)=1}}^{r^2} \left|T(a/r^2)\right|^2 \ll (RK)^\varepsilon \left(R^3 + K\right) A$$

(which corresponds to shape of the classical large sieve inequality). In this case we obtain that for any fixed $\varepsilon > 0$ there exists $\delta > 0$ such that for all $p \sim P$ except for $O(P^{1-\delta})$ the bound

$$\max_{\gcd(a,p)=1} |S_p(a, N_p)| \le N^{1/2} p^{1/3+\varepsilon},$$

holds for any sequence $N_p \sim N$, with some $N \ge p$, which is stronger than (1).

Finally, we notice that although Theorem 13 shows the existence of small primitive roots modulo p, the only known bound of multiplicative character sums (2) is nontrivial only for $N \ge p^{5/4+\varepsilon}$. Estimating shorter sums, either for every p or on average over p, is an interesting open question.

Acknowledgement

The author is grateful to Arne Winterhof for the careful reading of the manuscript and many useful discussions.

During the preparation of this paper, the author was supported in part by the Australian Research Council Grant DP1092835.

References

[1] H. Aly and A. Winterhof, 'Boolean functions derived from Fermat quotients', *Cryptography and Communications*, (to appear).

[2] S. Baier and L. Zhao, 'Large sieve inequality with characters for powerful moduli', *Intern. J. Number Theory*, **1** (2005) 265–280.

[3] S. Baier and L. Zhao, 'An improvement for the large sieve for square moduli', *J. Number Theory*, **128** (2008), 154–174.

[4] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan Math. J.*, **59** (2010), 313–328.

[5] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2008** (2008), Article ID rnn090, 1–29.

[6] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Corrigenda to: Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2009** (2009), 3146-3147.

[7] Z. Chen, A. Ostafe and A. Winterhof, 'Structure of pseudorandom numbers derived from Fermat quotients', *Lect. Notes in Comp. Sci.*, vol. 6087, Springer-Verlag, Berlin, 2010, 73–85.

[8] R. Ernvall and T. Metsänkylä, 'On the p-divisibility of Fermat quotients', *Math. Comp.*, **66** (1997), 1353–1365.

[9] M. Z. Garaev, 'Character sums in short intervals and the multiplication table modulo a large prime', *Monat. Math.*, **148** (2006), 127–138.

[10] D. Gomez and A. Winterhof, 'Multiplicative character sums of Fermat quotients and pseudorandom sequences', *Period. Math. Hungar.*, (to appear).

[11] A. Granville, 'Some conjectures related to Fermat's Last Theorem', *Number Theory*, W. de Gruyter, NY, 1990, 177–192.

[12] A. Granville, 'On pairs of coprime integers with no large prime factors', *Expos. Math.*, **9** (1991), 335–350.

[13] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[14] D. R. Heath-Brown, 'An estimate for Heilbronn's exponential sum', *Analytic Number Theory: Proc. Conf. in honor of Heini Halberstam*, Birkhäuser, Boston, 1996, 451–463.

[15] Y. Ihara, 'On the Euler-Kronecker constants of global fields and primes with small norms', *Algebraic Geometry and Number Theory*, Progress in Math., Vol. 850, Birkhäuser, Boston, Cambridge, MA, 2006, 407–451.

[16] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[17] A. A. Karatsuba, 'The distribution of values of Dirichlet characters on additive sequences', *Doklady Acad. Sci. USSR*, **319** (1991), 543–545 (in Russian).

[18] A. A. Karatsuba, *Basic analytic number theory*, Springer-Verlag, 1993.

[19] H. W. Lenstra, 'Miller's primality test', *Inform. Process. Lett.*, **8** (1979), 86–88.

[20] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, 1983.

[21] A. Ostafe and I. E. Shparlinski, 'Pseudorandomness and dynamics of Fermat quotients', *SIAM J. Discr. Math.*, **25** (2011), 50–71.

[22] I. E. Shparlinski, 'Character sums with Fermat quotients', *Quart. J. Math.*, (to appear).

[23] I. E. Shparlinski, 'Bounds of multiplicative character sums with Fermat quotients of primes', *Bull. Aust. Math. Soc.*, (to appear).

[24] I. E. Shparlinski, 'On the value set of Fermat quotients', *Proc. Amer. Math. Soc.*, (to appear).

[25] L. Zhao, 'Large sieve inequality for characters to square moduli', *Acta Arith.*, **112** (2004), 297–308.